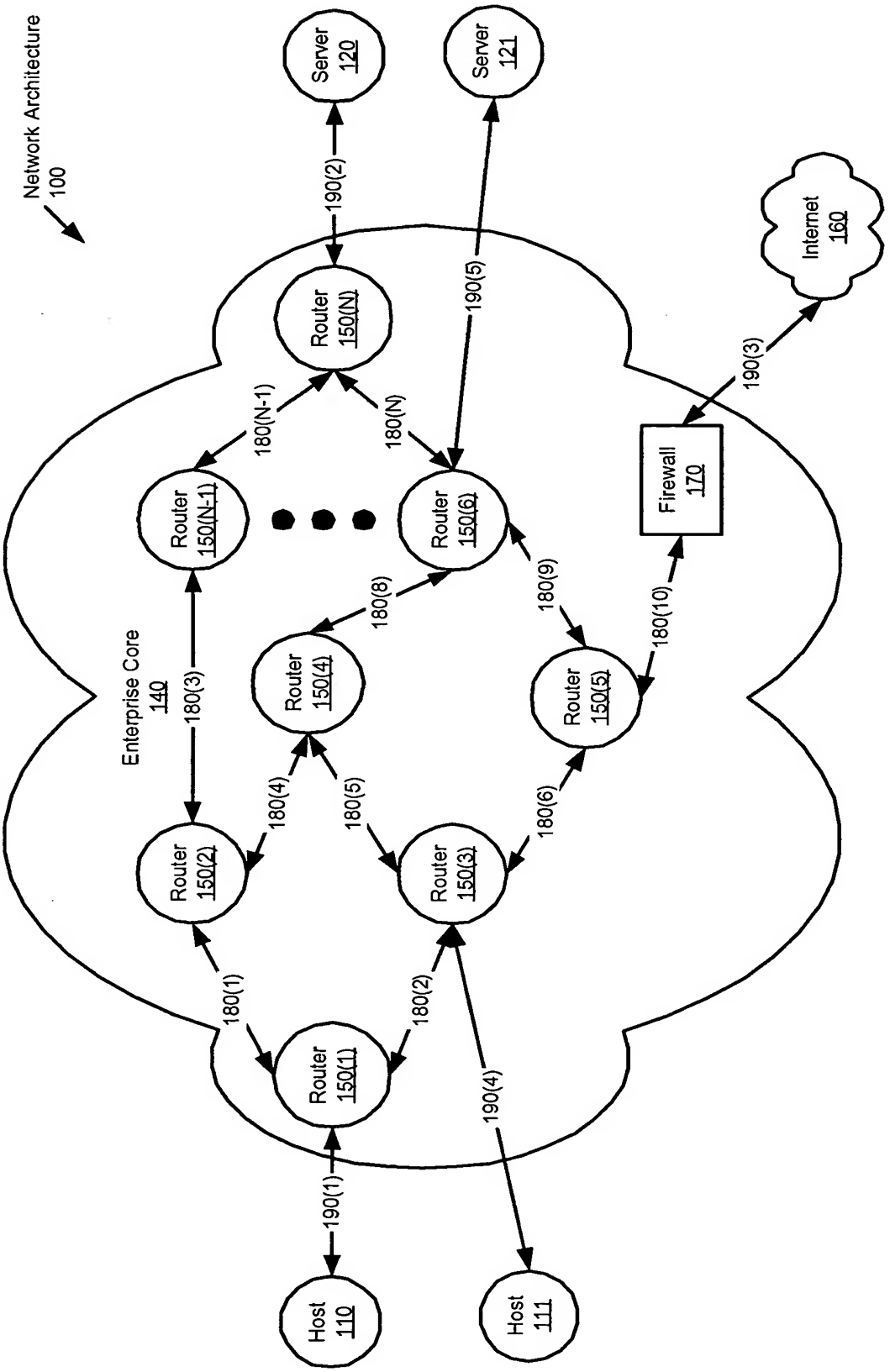
Network Architecture
100
Server
120
Server
121
Internet
160
Router
150(N)
Router
150(N-1)
Router
150(6)
Firewall
170
Router
150(4)
Router
150(5)
Router
150(2)
Router
150(3)
Router
150(1)
Enterprise Core
140
Host
110
Host
111
190(1)
190(2)
190(3)
190(4)
190(5)
180(1)
180(2)
180(3)
180(4)
180(5)
180(6)
180(8)
180(9)
180(10)
180(N-1)
180(N)

*Fig. 1*

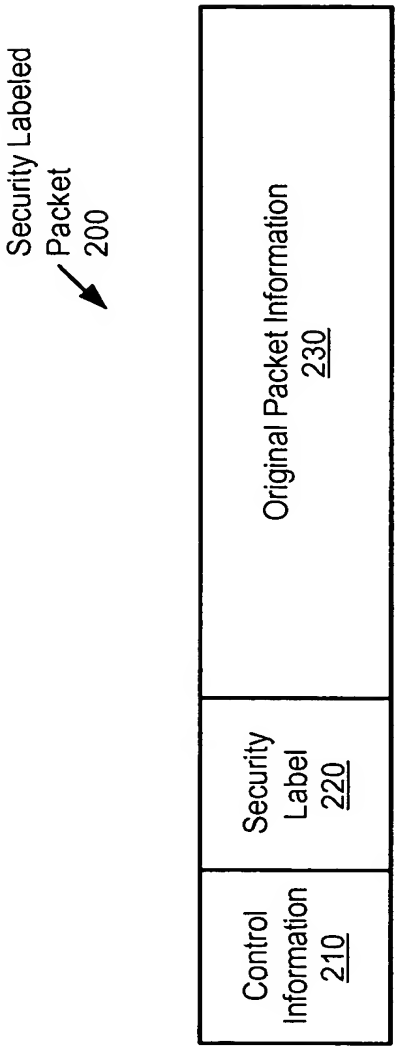
Security Labeled Packet 200
Control Information 210
Security Label 220
Original Packet Information 230

*Fig. 2*

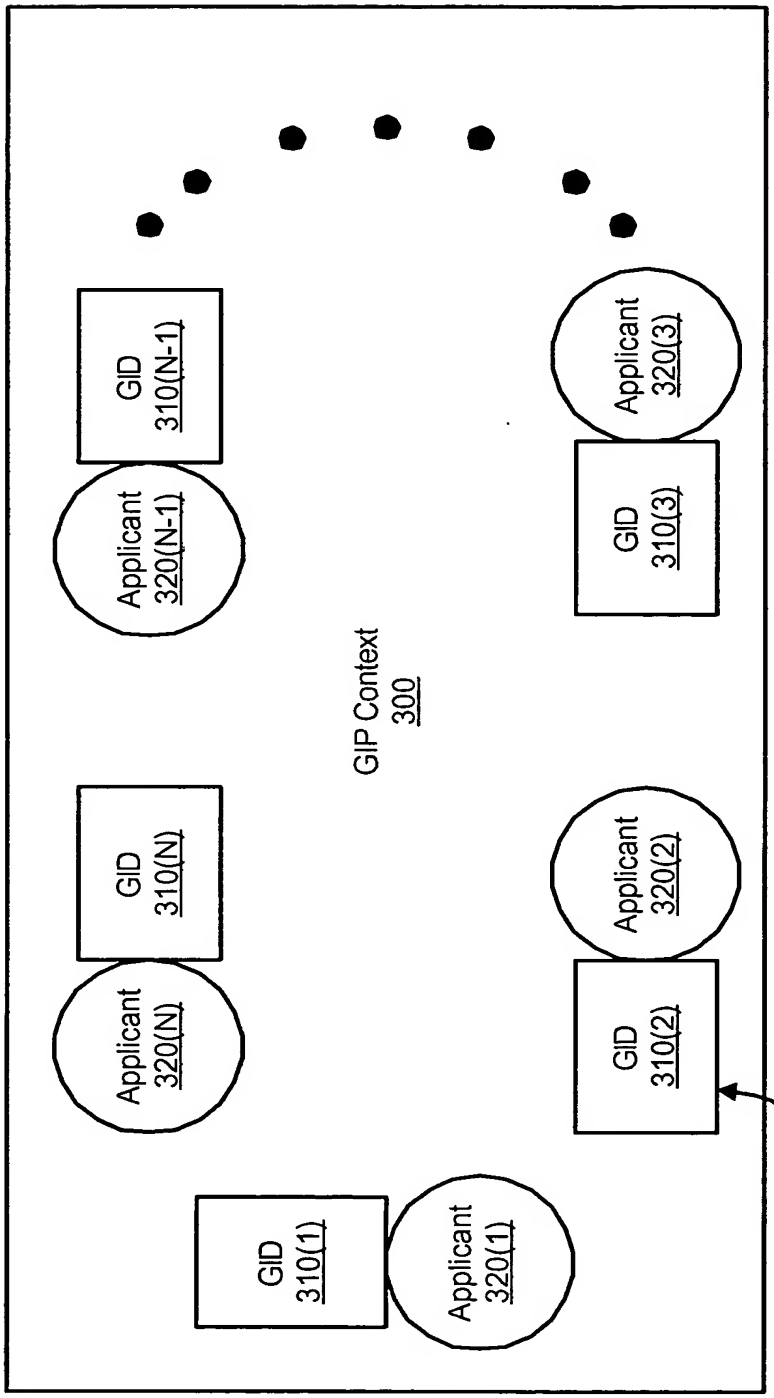
GIP Context
300
GID
310(1)
Applicant
320(1)
GID
310(2)
Applicant
320(2)
330
Join
GID
310(N)
Applicant
320(N)
GID
310(N-1)
Applicant
320(N-1)
GID
310(3)
Applicant
320(3)

*Fig. 3*

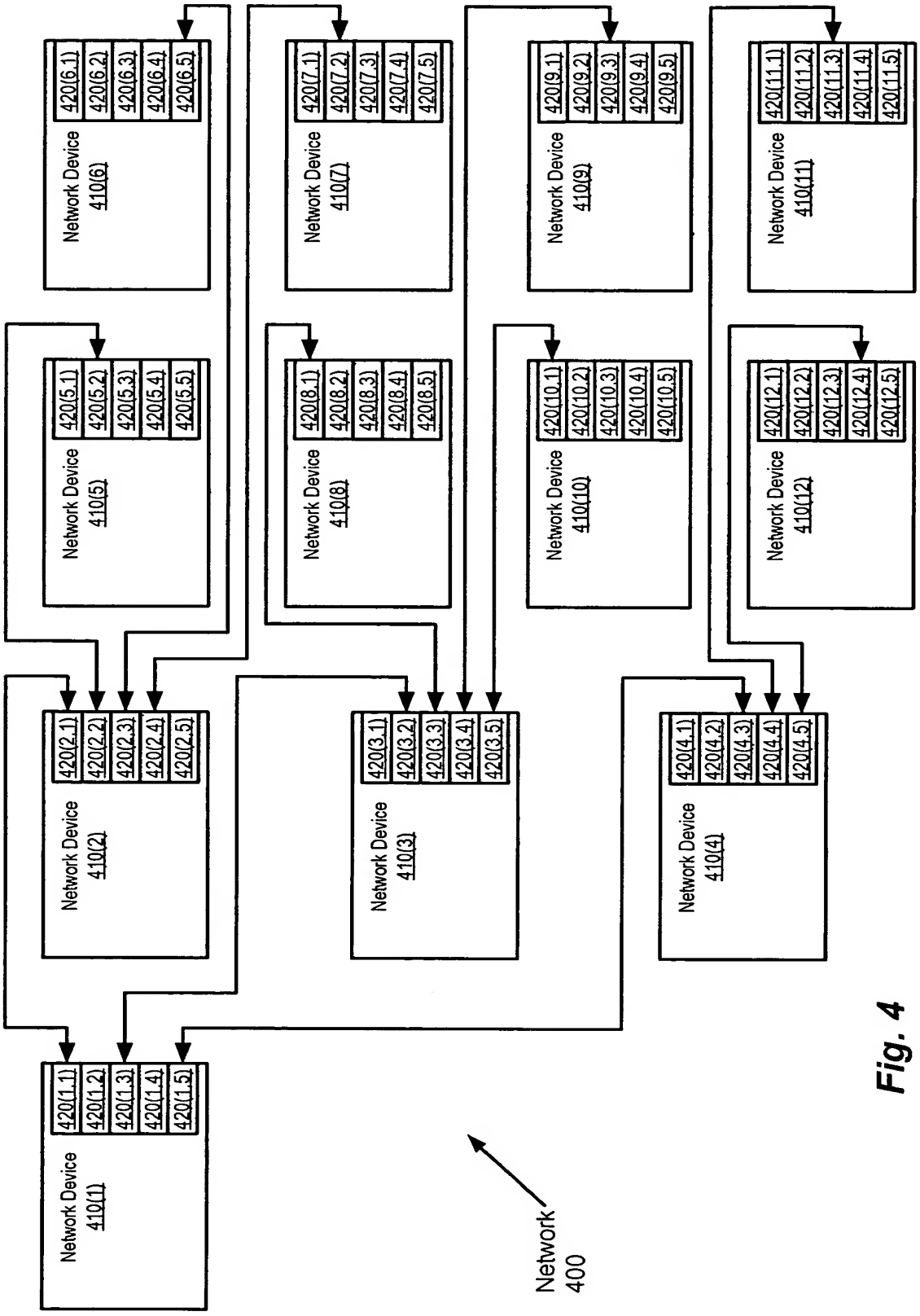
Network Device 410(1)
420(1.1) 420(1.2) 420(1.3) 420(1.4) 420(1.5)
Network Device 410(2)
420(2.1) 420(2.2) 420(2.3) 420(2.4) 420(2.5)
Network Device 410(3)
420(3.1) 420(3.2) 420(3.3) 420(3.4) 420(3.5)
Network Device 410(4)
420(4.1) 420(4.2) 420(4.3) 420(4.4) 420(4.5)
Network Device 410(5)
420(5.1) 420(5.2) 420(5.3) 420(5.4) 420(5.5)
Network Device 410(6)
420(6.1) 420(6.2) 420(6.3) 420(6.4) 420(6.5)
Network Device 410(7)
420(7.1) 420(7.2) 420(7.3) 420(7.4) 420(7.5)
Network Device 410(8)
420(8.1) 420(8.2) 420(8.3) 420(8.4) 420(8.5)
Network Device 410(9)
420(9.1) 420(9.2) 420(9.3) 420(9.4) 420(9.5)
Network Device 410(10)
420(10.1) 420(10.2) 420(10.3) 420(10.4) 420(10.5)
Network Device 410(11)
420(11.1) 420(11.2) 420(11.3) 420(11.4) 420(11.5)
Network Device 410(12)
420(12.1) 420(12.2) 420(12.3) 420(12.4) 420(12.5)
Network 400

*Fig. 4*

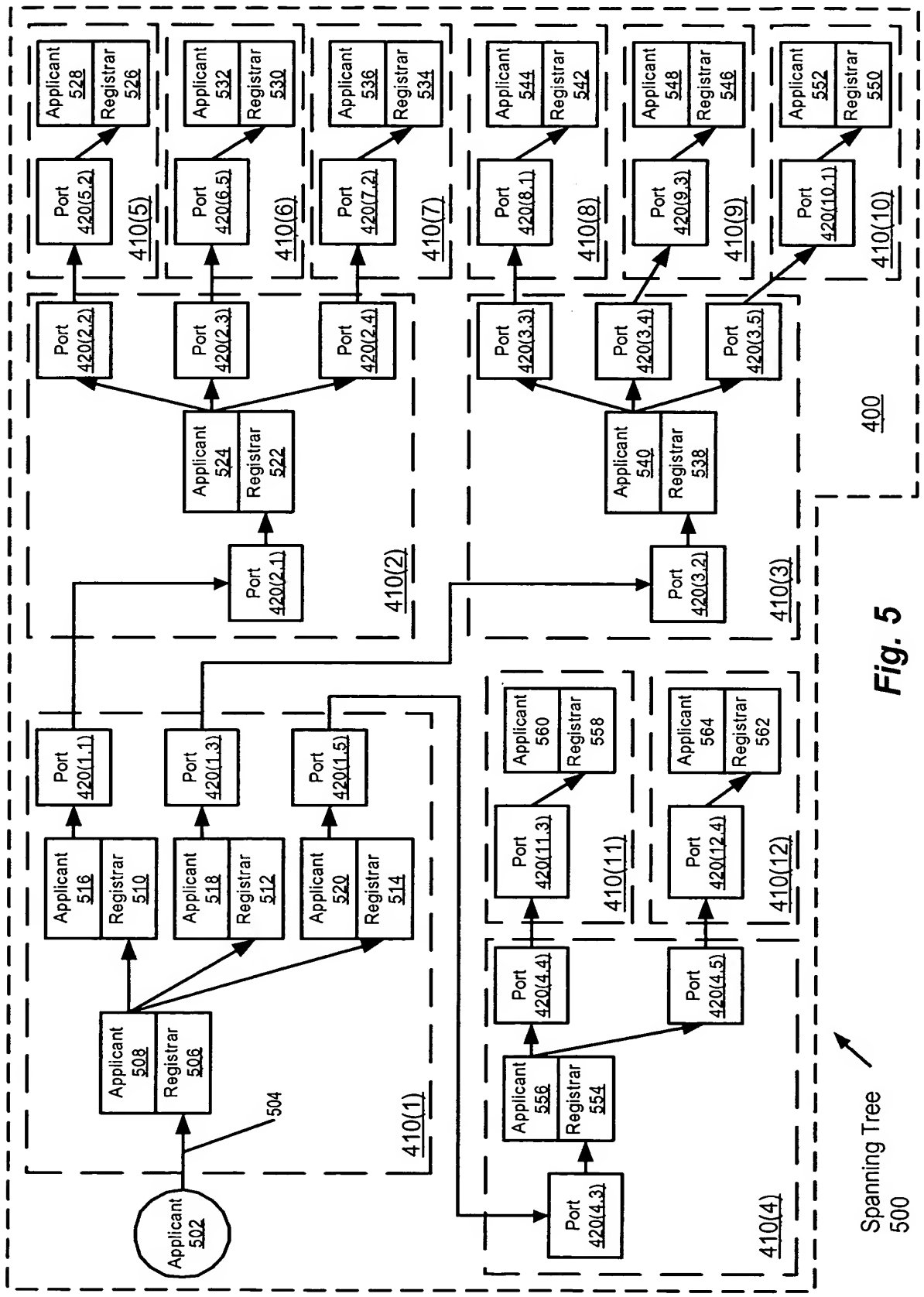
Applicant 502
504
Applicant 508
Registrar 506
Applicant 516
Registrar 510
Applicant 518
Registrar 512
Applicant 520
Registrar 514
Port 420(1.1)
Port 420(1.3)
Port 420(1.5)
Port 420(2.1)
Applicant 524
Registrar 522
Port 420(2.2)
Port 420(2.3)
Port 420(2.4)
Applicant 528
Registrar 526
Applicant 532
Registrar 530
Applicant 536
Registrar 534
Port 420(5.2)
Port 420(6.5)
Port 420(7.2)
Port 420(3.2)
Applicant 540
Registrar 538
Port 420(3.3)
Port 420(3.4)
Port 420(3.5)
Applicant 544
Registrar 542
Applicant 548
Registrar 546
Applicant 552
Registrar 550
Port 420(8.1)
Port 420(9.3)
Port 420(10.1)
Port 420(4.3)
Applicant 556
Registrar 554
Port 420(4.4)
Port 420(4.5)
Applicant 560
Registrar 558
Applicant 564
Registrar 562
Port 420(11.3)
Port 420(12.4)
410(1)
410(2)
410(3)
410(4)
410(5)
410(6)
410(7)
410(8)
410(9)
410(10)
410(11)
410(12)
400
Spanning Tree 500

Fig. 5

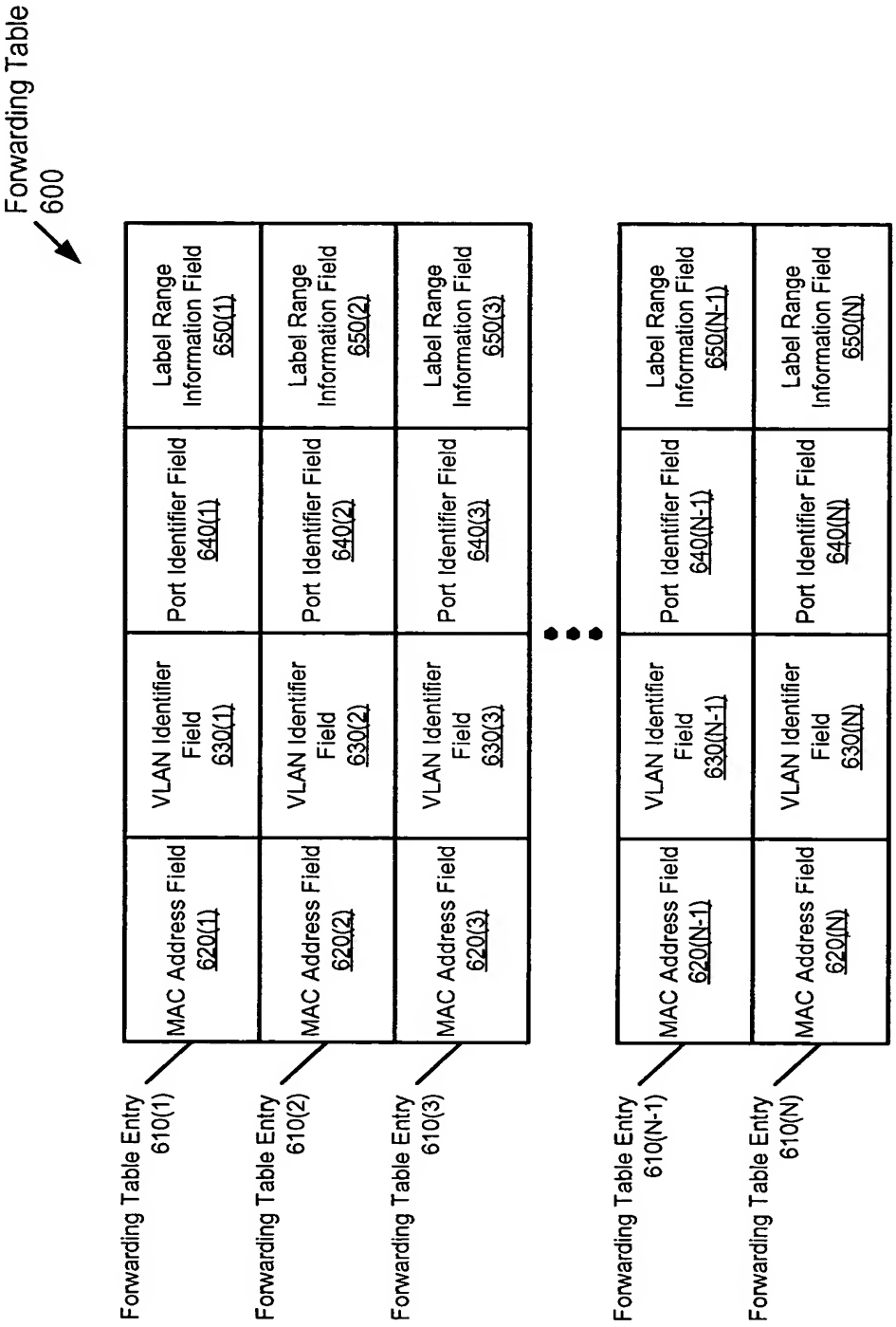
Forwarding Table
600
MAC Address Field 620(1)
VLAN Identifier Field 630(1)
Port Identifier Field 640(1)
Label Range Information Field 650(1)
MAC Address Field 620(2)
VLAN Identifier Field 630(2)
Port Identifier Field 640(2)
Label Range Information Field 650(2)
MAC Address Field 620(3)
VLAN Identifier Field 630(3)
Port Identifier Field 640(3)
Label Range Information Field 650(3)
MAC Address Field 620(N-1)
VLAN Identifier Field 630(N-1)
Port Identifier Field 640(N-1)
Label Range Information Field 650(N-1)
MAC Address Field 620(N)
VLAN Identifier Field 630(N)
Port Identifier Field 640(N)
Label Range Information Field 650(N)
Forwarding Table Entry 610(1)
Forwarding Table Entry 610(2)
Forwarding Table Entry 610(3)
Forwarding Table Entry 610(N-1)
Forwarding Table Entry 610(N)

*Fig. 6*

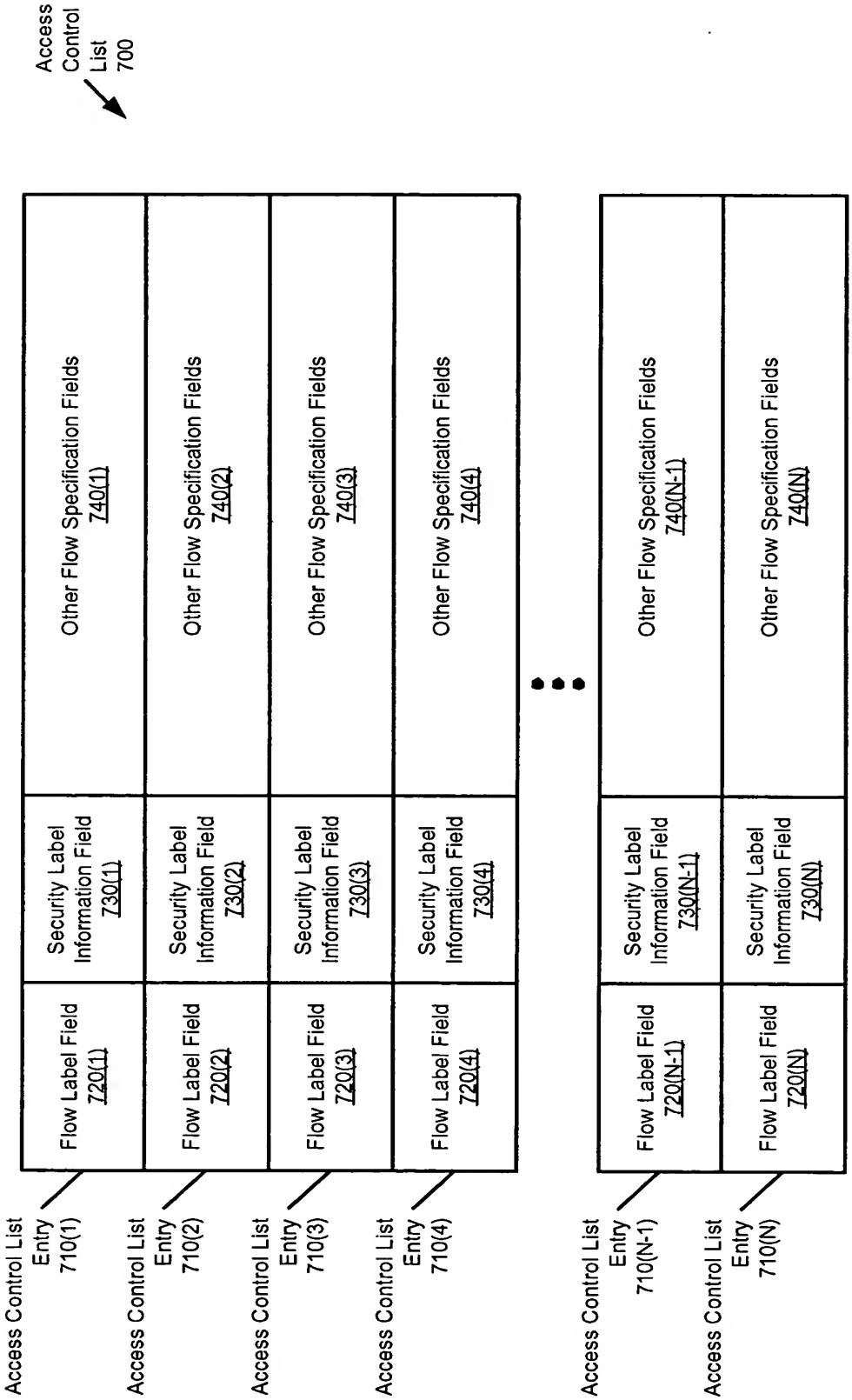
Access Control List 700
Access Control List Entry 710(1)
Flow Label Field Z20(1)
Security Label Information Field Z30(1)
Other Flow Specification Fields Z40(1)
Access Control List Entry 710(2)
Flow Label Field Z20(2)
Security Label Information Field Z30(2)
Other Flow Specification Fields Z40(2)
Access Control List Entry 710(3)
Flow Label Field Z20(3)
Security Label Information Field Z30(3)
Other Flow Specification Fields Z40(3)
Access Control List Entry 710(4)
Flow Label Field Z20(4)
Security Label Information Field Z30(4)
Other Flow Specification Fields Z40(4)
Access Control List Entry 710(N-1)
Flow Label Field Z20(N-1)
Security Label Information Field Z30(N-1)
Other Flow Specification Fields Z40(N-1)
Access Control List Entry 710(N)
Flow Label Field Z20(N)
Security Label Information Field Z30(N)
Other Flow Specification Fields Z40(N)

*Fig. 7*

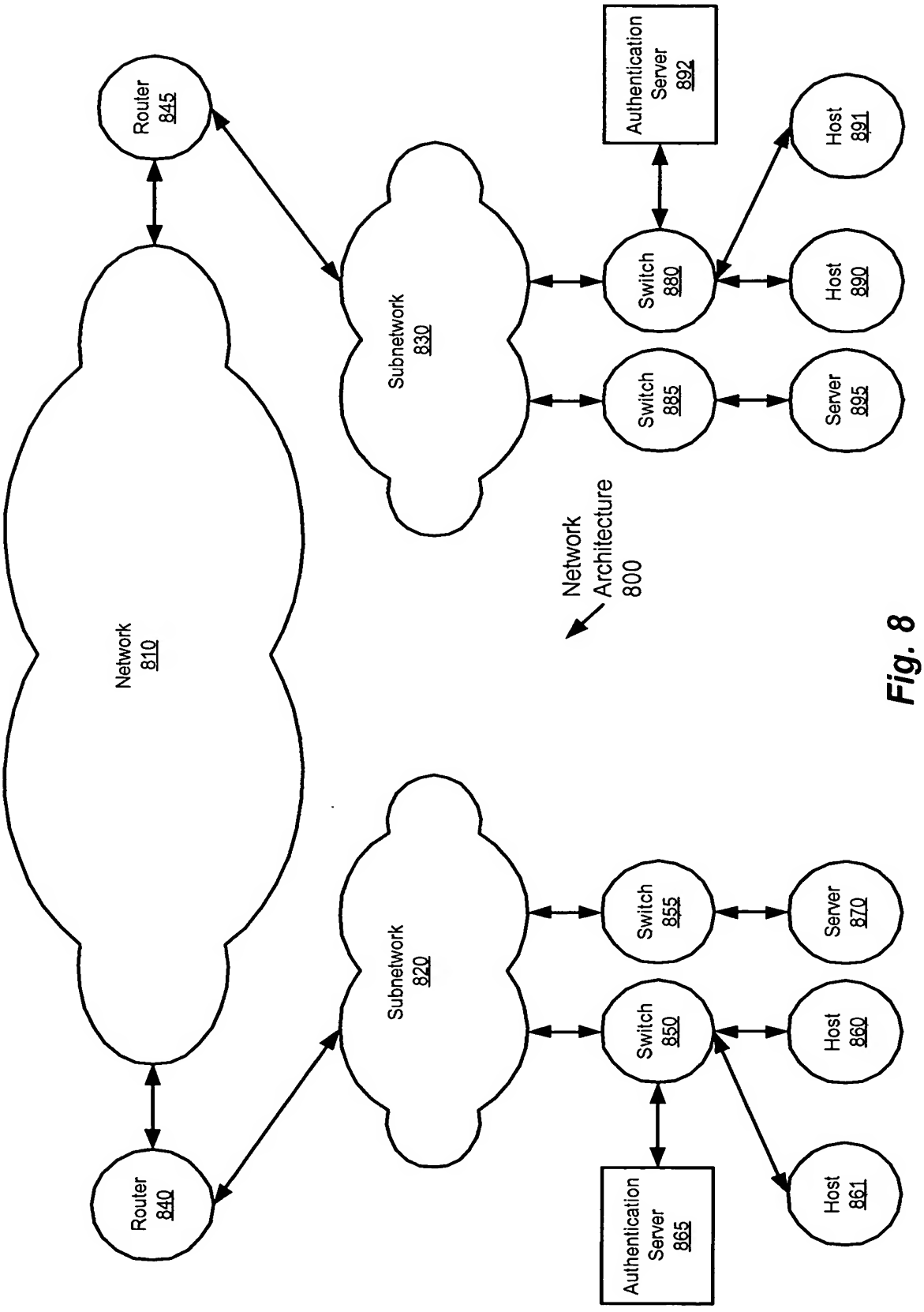
Network
810
Router
845
Router
840
Subnetwork
830
Subnetwork
820
Authentication
Server
892
Switch
880
Switch
885
Host
891
Host
890
Server
895
Switch
855
Switch
850
Server
870
Host
860
Host
861
Authentication
Server
865
Network
Architecture
800

*Fig. 8*

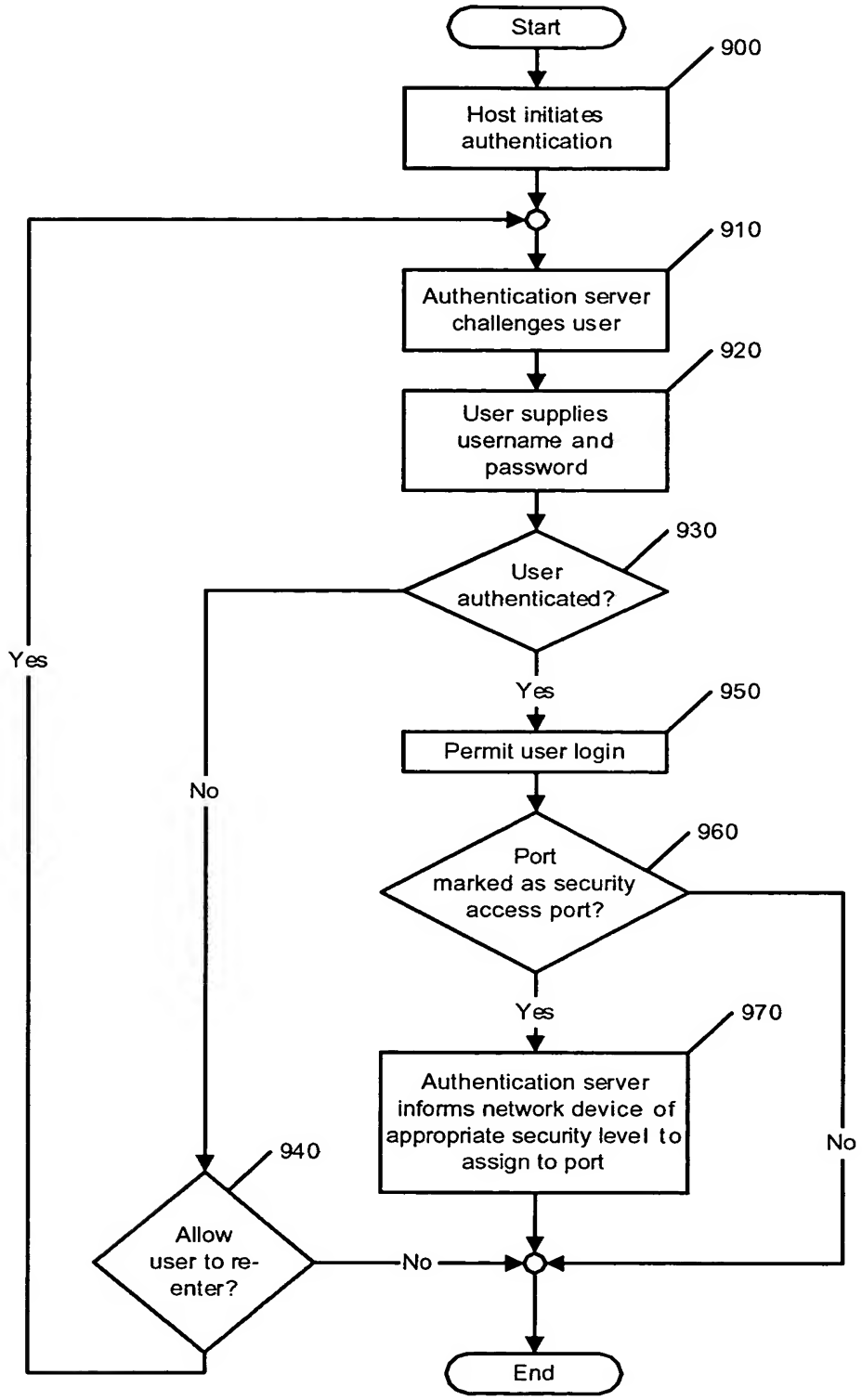
Start
900
Host initiates authentication
910
Authentication server challenges user
920
User supplies username and password
930
User authenticated?
Yes
No
950
Permit user login
960
Port marked as security access port?
Yes
No
970
Authentication server informs network device of appropriate security level to assign to port
940
Allow user to re-enter?
No
Yes
End

*Fig. 9*

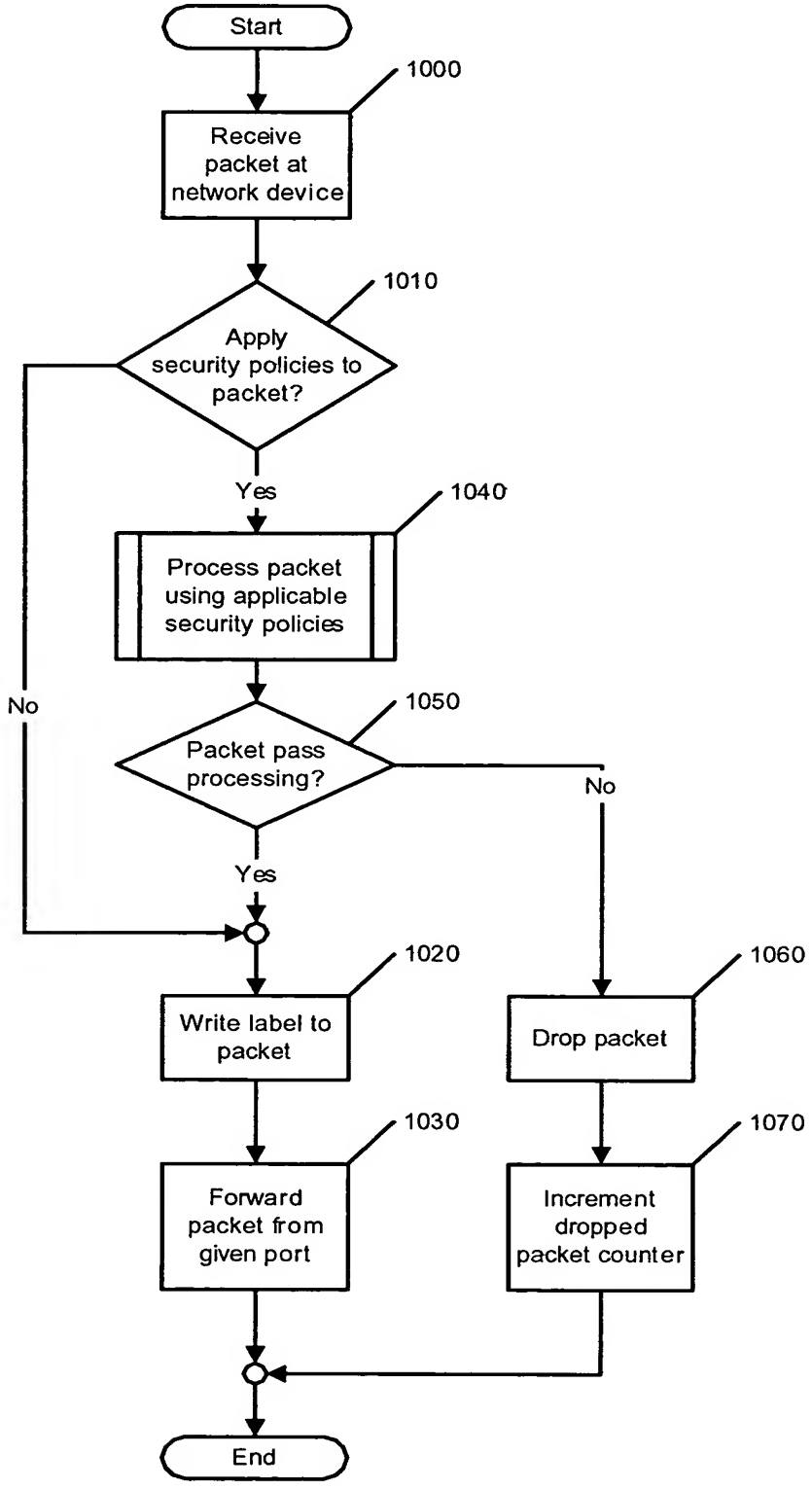
Start
1000
Receive packet at network device
1010
Apply security policies to packet?
Yes
No
1040
Process packet using applicable security policies
1050
Packet pass processing?
Yes
No
1020
Write label to packet
1030
Forward packet from given port
1060
Drop packet
1070
Increment dropped packet counter
End

*Fig. 10*

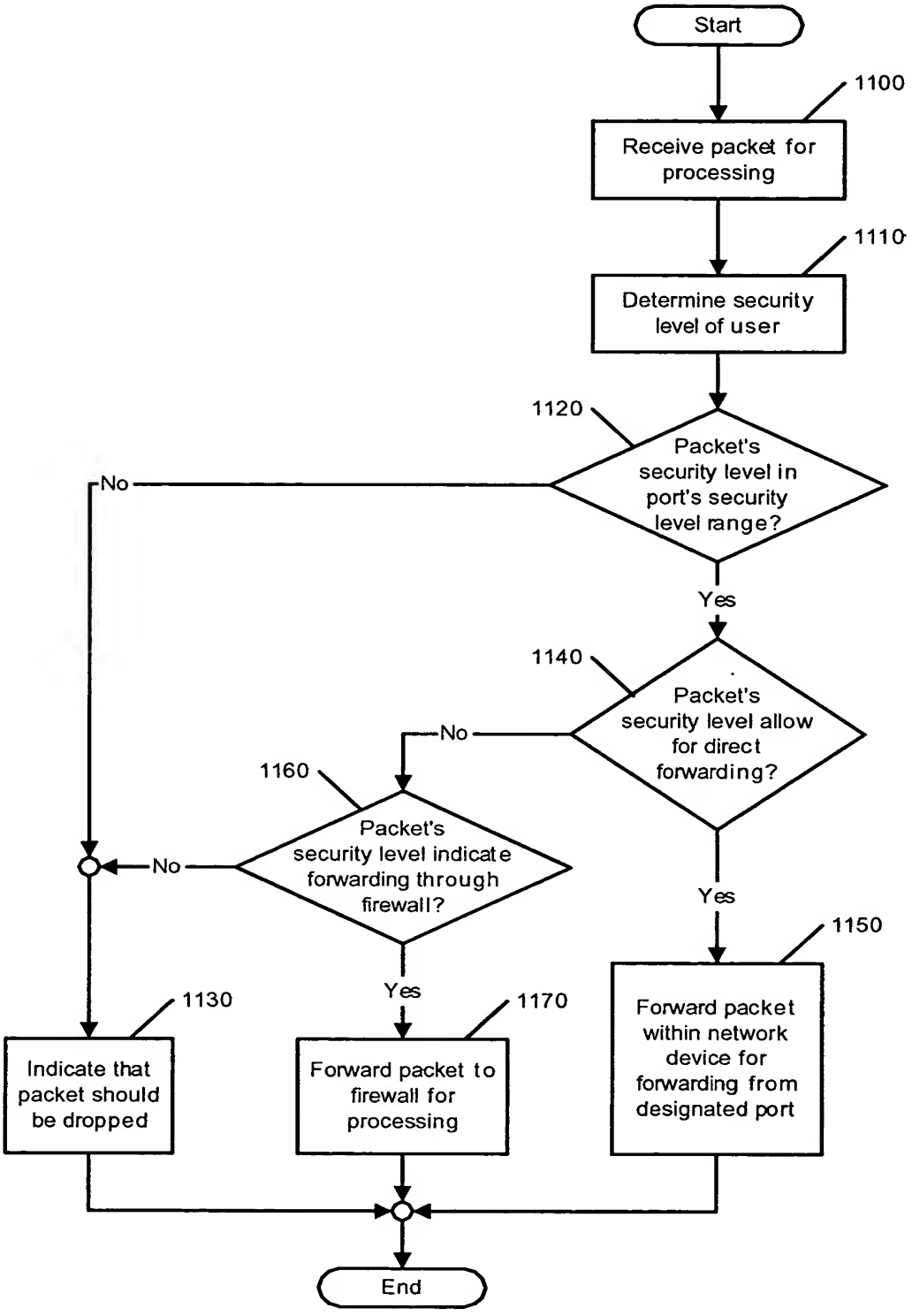
Start
1100
Receive packet for processing
1110
Determine security level of user
1120
Packet's security level in port's security level range?
No
Yes
1140
Packet's security level allow for direct forwarding?
No
1160
Packet's security level indicate forwarding through firewall?
No
Yes
Yes
1150
Forward packet within network device for forwarding from designated port
1130
Indicate that packet should be dropped
1170
Forward packet to firewall for processing
End

*Fig. 11*

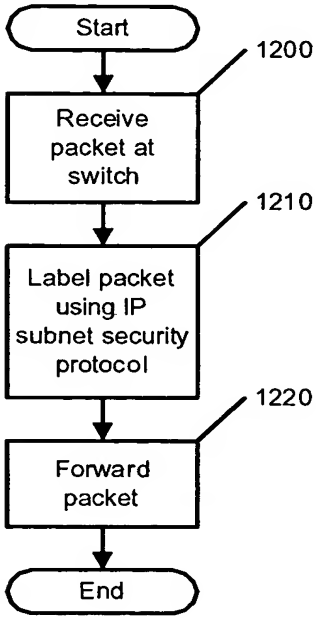


*Fig. 12A*

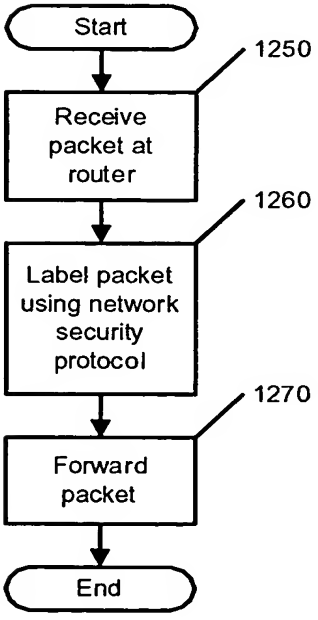


*Fig. 12B*

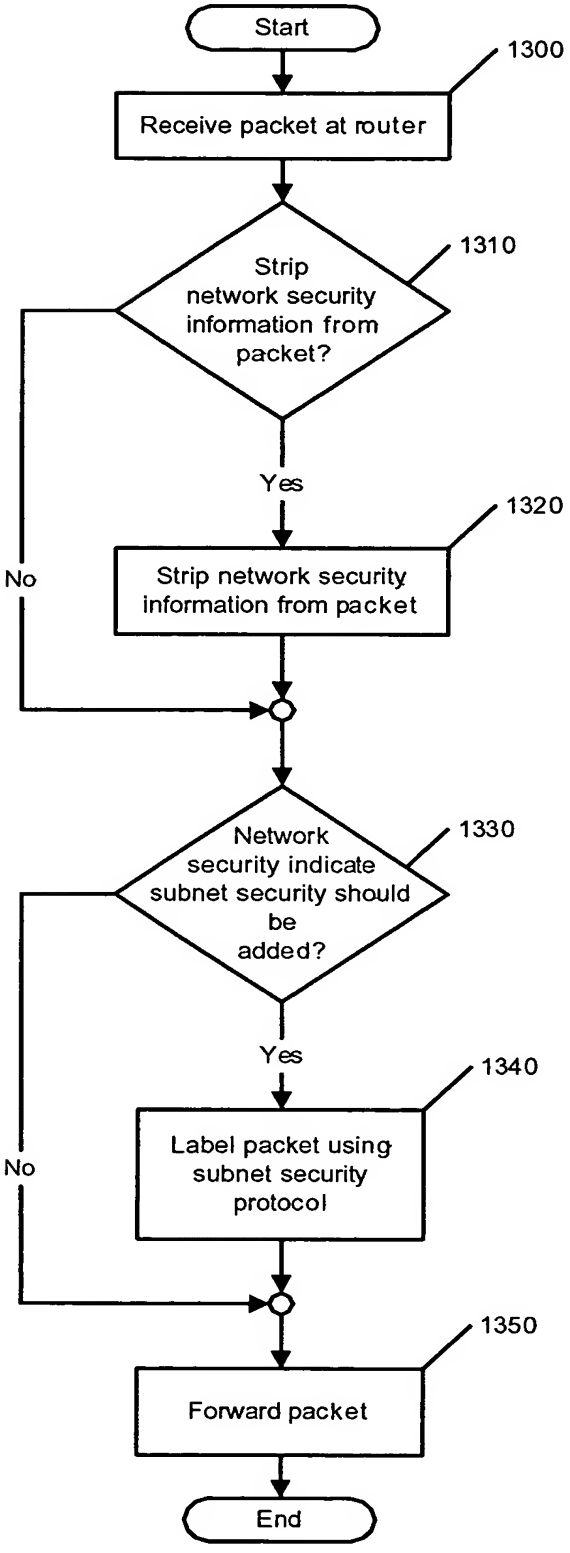
Start
1300
Receive packet at router
1310
Strip network security information from packet?
Yes
No
1320
Strip network security information from packet
1330
Network security indicate subnet security should be added?
Yes
No
1340
Label packet using subnet security protocol
1350
Forward packet
End

*Fig. 13*

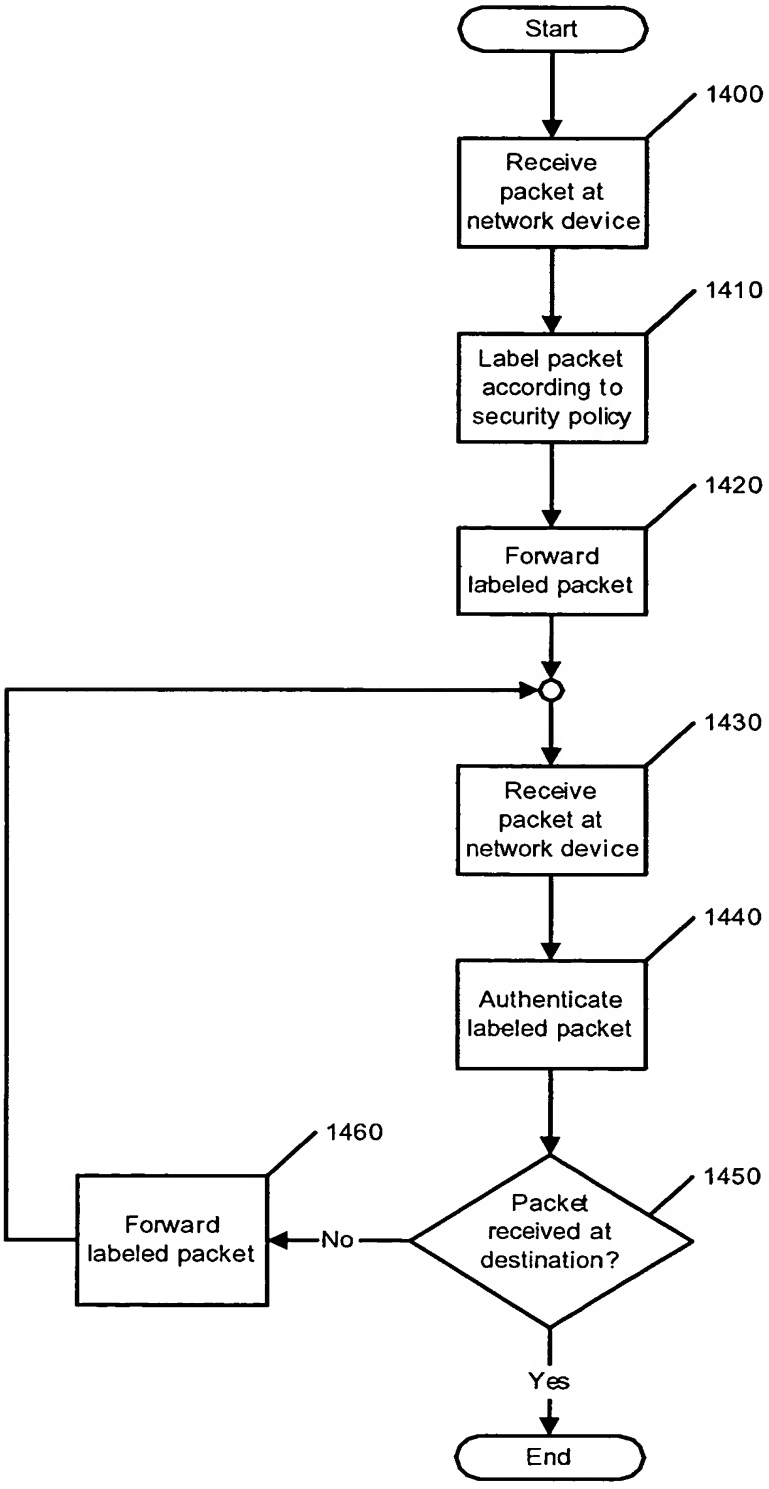
Start
1400
Receive packet at network device
1410
Label packet according to security policy
1420
Forward labeled packet
1430
Receive packet at network device
1440
Authenticate labeled packet
1450
Packet received at destination?
No
1460
Forward labeled packet
Yes
End

*Fig. 14*